UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/535,363	05/18/2005	Christian Kollmitzer	SONN:069US/10503277	7070

32425 7590 12/16/2009

FULBRIGHT & JAWORSKI L.L.P.
600 CONGRESS AVE.
SUITE 2400
AUSTIN, TX 78701

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2437	

MAIL DATE	DELIVERY MODE
12/16/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/535,363	KOLLMITZER, CHRISTIAN	
	Examiner	Art Unit	
	MICHAEL PYZOCHA	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 November 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *11-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *11-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Amendment filed 11/02/2009 has been received and considered.

2. Claims 11-21 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim11-16 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elliot (Building the quantum network) in view of Buer et al. (US 20040005061).

As per claim 11, Elliott discloses a communication system using quantum cryptography comprising: subscriber stations connected to one or more quantum channels (see the Private Enclaves in Figures 1 and 5 and the first paragraph of section 3 on page 46.4); one or more quantum-cryptographic device associated with the one or more quantum channels for generating a quantum key during use (see the QKD Endpoints of Figures 1 and 5 and page 46.9); and several interconnected switching stations that, during use, communicate via first lines, using encryption agreed upon (see page 46.9); wherein, during use, the subscriber stations are connected to the switching stations via the one or more quantum channels that generate a respective temporary quantum key and are adapted to communicate via second public lines using the quantum key, and wherein the first lines are distinct from the second lines and are a

priori secure lines to transmit the generated quantum key from one switching station to another and to another subscriber station (see pages 46.4-46.5 and 46.8-46.9).

Elliot fail to disclose that the switching stations communicate with each other over public lines using agreed upon encryption.

However, Buer et al. teaches the use of public lines which are a priori secured using agreed upon encryption to exchange encryption keys (see paragraphs [0142] and [1045] where the KEKs, or key encryption keys, encrypt the different encryption keys).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to substitute the known key exchange method of Buer et al. in place of the key exchange method of the Elliot system.

Motivation to do so would have been to allow different encryption keys to be secured using different KEKs (see Buer et al. paragraph [0145]).

As per claims 12-14, the modified Elliott and Buer et al. system discloses the switching stations have a source of photons and a photon detector and the subscriber stations comprise a photon detector (see Elliot pages 46.4-46.5 and 46.8-46.9 where each node must be able to create and detect photons to be able to communicate of a quantum channel).

As per claim 15, the modified Elliott and Buer et al. system discloses the switching stations are interconnected at least partially by point-to-point links (see Elliot page 46.4 and 46.9 and Figures 1 and 5).

As per claim 16, the modified Elliott and Buer et al. system discloses the switching stations are at least partially hierarchically interconnected (see Elliot Figure 5 and page 46.9).

As per claim 21, the modified Elliott and Buer et al. system discloses wherein, during use, authentication data transmitted between the switching stations are checked by the switching stations prior to the establishment of a communication between subscriber stations (see Elliot page 46.3 Authentication).

5. Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Elliott and Buer et al. system as applied to claim 11 above, in view of Elliot (US 7457416).

As per claims 17 and 18, the modified Elliott and Buer et al. system discloses generating key bits between subscriber stations and their associated switching stations after a request for communication has been transmitted (see Elliot pages 46.4-46.5 and 46.8-46.9), but fails to explicitly disclose generating a separate bit sequence and wherein, during use, a switching station associated with a called subscriber station generates a third key bit sequence from the key bit sequences generated via the quantum channels and transmits this third key bit sequence to the called subscriber station which, using the key bit sequence known to it and generated by it together with the associated switching station, from the third key bit sequence generates the key bit sequence generated on the part of the calling subscriber station, which then finally is used as a mutual key for the communication between the subscriber stations.

However, Elliott teaches such a quantum key agreement protocol (see FIG. 4 and column 6 line 48 through column 7 line 38).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the specific key agreement protocol of Elliott in the modified Elliott and Buer et al. system.

Motivation to do so would have been to allow for user devices to share a common secret key over an insecure network (see Elliott column 2 lines 41-44).

6. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Elliott and Buer et al. system as applied to claim 11 above, in view of Menezes et al. (Handbook of Applied Cryptography).

As per claim 19, the modified Elliott and Buer et al. system fails to explicitly disclose discarding the quantum keys at the end of a communication.

However, Menezes et al. teaches discarding a key after a communication (see page 553).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to discard the quantum key of the modified Elliott and Buer et al. system after a communication.

Motivation to do so would have been to limit the exposure of the key (see Menezes et al. page 553).

7. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Elliott and Buer et al. system as applied to claim 11 above, in view of Townsend et al. (US 5850441).

As per claim 20, the modified Elliott and Buer et al. system fails to explicitly disclose discarding the quantum keys at the end of communications of when eavesdropping is detected.

However, Townsend et al. teaches such discarding (see column 3 lines 29-48).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to discard the keys of the modified Elliott and Buer et al. system.

Motivation, as recognized by one of ordinary skill in the art, would have been to protect the security of the system.

Response to Arguments

8. Applicant's arguments with respect to claims 11-21 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Hughes teaches exchanging quantum keys over public lines and Matyas teaches exchanging keys over public lines using encryption.

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 3:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Pyzocha/
Primary Examiner, Art Unit 2437